S2G

System Security | Research group

Research Group Strategy

Excellence in System Security

Motto:

Better secure than sorry! Follow our research and advise in system security.

Mission:

Our mission is to ensure that systems in the digital society are resilient against cyber-attacks and fulfill essential security and privacy requirements. The Systems that we focus our research on go beyond the classic ICT perspective and include societal, economical and human factors.

Values:

Quality, Internationalization, Innovation, Visibility

Objectives:

Our research objectives are to develop models, methods, techniques and tools that can be used for:

- building secure systems
- evaluating and assessing the security of systems
- enhancing the security of systems
- training and educating users and organizations to understand and apply security methods and adversarial thinking

Vision

Modern systems constantly become more digitally intensive, such as with Smart Grids, Smart Homes, or eHealth. However, this digitalization also increases the number of security prone systems that sustain critical human activities, hence more dangerous systems. This is exacerbated by the IoT revolution, with cheap miniaturization of computing becoming included in most of our daily tools and services. These digital dangers scare the general public and authorities, who push back and slow down the technological innovation and adoption. To resolve this conflict we work to increase the level of system security that the new digital solutions provide, so to raise the trust that the society has in its complex digitalized infrastructures.

Our vision is for security to become an integral necessary part of every modern digital system development process. In metaphorical terms, we want Security to be for Systems development, the same as fire safety is for architecture or as food safety is for restaurants. To achieve this, system security research is needed at all levels, from the usability of security for end users, to secure development processes, security training platforms, powerful security tools, and even formal methods for security assurance and verification. Positive examples such as the DevSecOps drive for more security tools and training throughout the software development life-cycle or the GDPR regulations for privacy, only support and encourage our vision of a more secure digital society. Our efforts try to steer society away from the current “security after the fact” practices and into a “security built in” mentality.

Activities

Our activities are roughly divided into those pertaining to Research, Innovation, Dissemination, Societal responsibilities, and Teaching.

Research

The research activities of our group are both theoretical as well as application oriented, and are conducted in areas such as secure software development life-cycle, security assurance and maturity modeling, vulnerability, threat and risk analysis, DevOps security, modeling and verification of security protocols, model-driven security, human aspects of security, or security training, awareness and education. These areas of our activity are subject to change – and rightfully so – following the highly dynamic problem landscape in security research.

Indicators for research:

- publication points per full time employee
  (in accordance with the indicators from the national and university levels)
- indicators used internally in the group include various other important research activities:
  - # awards (e.g., best paper, best talk, best demo, etc),
  - # publications in venues that are highly ranked in a specific research field, according both to known rankings as well as own experience of quality research in the respective field.

Innovation

Our innovation activities mostly deal with bringing into practice ideas and results from the research world, both from our own research results, but also other’s. There are largely two types of innovation activities that we engage in:

I. *Innovation driven by the researchers.*
   This is some of the most common type of innovation found in the academia, and the most forgotten, or overlooked, in the society and industry at large. These innovation activities usually

demonstrate applicability or implementability of a research idea. This is what Einstein did when he calculated the movements of Mercury or what Turing did when he detailed the designs of the Automatic Computing Engine based on the principles of his computational machines. These are the endeavors that researchers undertake after they have discovered something new, and often in security this involves implementing prototypes, or applying our algorithms. But research is too often much ahead of its time, so to say, compared to what the society and industry can comprehend, because research often tackles problems that are to come. Too often these prototyped/demonstrated solutions are re-invented and re-discovered several times over, as is the example with IoT (which academia has long studied under the name ubiquitous or pervasive systems) or with AI (which dates from the beginning of computer science, albeit under various different guises such as Support Decision Systems).

II. *Innovation asked by the society or industry.*
This is the type of innovation most commonly sought for and funded nowadays. These are activities working to solve a problem that an industry actor comes with. These are also the quite simple activities and often nonpublishable either because the solutions already exist in the research literature (but the industry needs them "translated") or because they are under some form of Intellectual Property Rights.

One focus for such innovation activities asked for by the society revolves around the NCR facilities (the Norwegian Cyber Range). Here is where industry actors come to test security ideas or to train on handling security challenges. The NCR provides the know-how from the research in a form that the industry can integrate in their daily practices. The NCR needs constant technological innovation activities to drive its technical infrastructure in order to keep up with the demands of the industry participants.

Indicators for innovation:

- funding per full time employee
  (in accordance with the indicators from the national and university levels)
  - value of funds from EU projects
  - value of funds from National or Regional projects
  - value of funds from Industry project (either contractual or bi-lateral)
- indicators used internally in the group include various other important innovation activities:
  - # startups and # startup ideas
    (shared with the TTO or other industry actors),
  - # student projects with innovation character
    (e.g., done for/together with a company, or contributing to prototyping a research idea, etc.)

    - # prototypes or # scientific tools maintained
      (it often takes long time and efforts before a research tool becomes mature enough for the industry to assimilate it)

Dissemination

Our dissemination activities are an integral part of our daily work and include everything involving telling others about our (or existing) research. These can be anything from classical presentations to research conferences, to specific research groups at other institutions (but also locally/nationally), to more prestigious invited talks and tutorials, or more mundane presentations to social or industrial actors where often the researcher's challenge is to simplify the language and the results in order to make it comprehensible for the audience (often the researcher needs to give up rigor and precision in favor of getting the message through).

Indicators for dissemination:

- # presentations to academic fora
  (in accordance with the indicators from the national and university levels)
- # invited talks and # tutorials given at academic fora or institutions (also counting in the ranking of the venue or the prestige of the institution)
- # presentations to industry or other social actors (with technical content)
- # media appearances (e.g., in newspapers, radio, TV, or media channels maintained by others)

Societal responsibilities

Our duty as academics is primarily (if not solely) to the society as we are fully paid by tax money (as opposed to private universities as, e.g., in the US). As such, we endeavor to solve research problems that society struggles with (currently or envisioned), while releasing our results back to the society in the form of publicly available articles. Therefore, one basic principle in our work is open access to our results (in one form or another, e.g., through authors' versions), as well as not engaging in work governed by non-disclosure agreements (as is often the case in industry).

Another basic responsibility that we have towards the society is to increase and drive the knowledge forward, at least keeping up to date with the international advances, which in our case are in the field of security and technology. Modern societies have a close correlation between wealth and standard of living on the one hand, and technological advancement and information sovereignty on the other (this is related to both national security or trade as well as industrial competitiveness).

Besides our production and dissemination of knowledge, including also higher education of the population, we also have minor societal responsibilities, as government employees, in the form of tasks where experts are needed. Such expert advise is asked for by various actors, and include activities such as appearance in court cases, participation in governmental expert panels, or evaluation and production of general interest reports for governmental actors or any other actors with an independent factor with a social agenda, such as for non-governmental organizations.

Indicators for societal activities:

- # participation in governmental panels, and other expert panels
- # participation in local events as experts, e.g., in law courts, advisory to NGOs, municipality decision making, etc.

Teaching

Our teaching activities are especially emphasized by the fact that our university is equally an institution for higher education as well as for research (e.g., the work division for a professor is usually divided into 40% – 40% – 20% respectively teaching – research – other duties usually related to administration and management aspects). One important aspect of our teaching activities is to be research-based. In Norway this means to expose the students also to current research on the topic of the course, besides the content being up to date with the latest advancements that the industry makes, often going beyond that.

Our supervision activities most of the time are on topics of direct relevance to some of our current research plans. Examples include various applications of our theories, or of related ones, or implementations of related prototypes, or studies and testing of research ideas and tools. All of these are, of course, with a grounding in the basic knowledge needed to understand the research topic. In this way the students experience both worlds, that of the research and that of learning basic principles not encountered in their studies.

One important activity is to teach the working population, that which is nowadays termed “life-long learning”. In this respect we develop smaller teaching modules, focused on target groups with needs that are different than those of students, both from a motivational as well as a background point of view. In the field of security, such life-long learning modules are not meant to re-educate someone, but more to bring up to date someone as the security field is very dynamic with both attacks and defense methods changing very often. Keeping the population up to date is paramount for security.

Indicators for dissemination:

- # supervised students (MSc and Bsc)
- # courses with at least one research-based lecture (e.g., MSc level courses normally have that)
- # students finishing our courses
(in accordance with the indicators from the national and university levels)

Plans

We are very good at producing quality research results, witnessed by our research articles published in highly ranked journals and venues. We are exceptionally active on the practical applications of our research, witnessed by the involvement in infrastructures such as the Norwegian Cyber Range, in development of security technology prototypes and startups, and in the number of student projects (BSc and MSc) which almost always involve quite concrete applications of our research.

We aim to continue these productive activities; and add those mentioned below.

Long term Plans (5 to 10 years)

Expand the S2G group with at least 3 permanent members. These new members should contribute to several of the core S2G research areas, but also contribute to enlarging S2G with additional research focus and expertise. Keeping a dynamic set of research topics is mandatory for a healthy research environment that wishes to be at the forefront of a constantly changing security research problems frontier.

Topics that are not currently core for our group but are envisioned to be relevant for us to engage more in are:

- AI and/for Security;
- Securing Cyber Physical systems;
- Quantum computing and/for Security;
- Sustainability and/of/in Security;

Five-years Plans

Contribute to making the Norwegian Cyber Range (NCR) a self-sustained research and innovation infrastructure with a substantial revenue produced from industrial clients and innovation activities, i.e., coming from outside the standard research funding. This own budget should not only contribute to the maintenance and operation of the NCR, but also to expansion of the physical and human infrastructure as well as adjacent satellite activities such as startups, events, student opportunities, or research activities.

To crystallize our ambitions and to have a drive and focus, the group should be involved in a large scale project one one or several of the group’s topics. One goal is to coordinate or be major partner in a project of the SFI/SFF type on the general topic of AI and/for Security.

2-years Plans

Develop, submit, and secure funding through projects in the areas of cyber ranges, security assurance, and human aspect in security. The funding would be sought mainly from the EU and from collaborative funding schemes where the NFR is partner. National funding is also encouraged, but as a second priority, as our constant endeavor is for forming and maintaining international collaborations. Our national collaborations network and visibility is already well established and is in a constant self-sustained dynamic; whereas the international level and competition is where we need to be pro-active in order to keep up with the constantly rising research quality standards and achievement expectations.

Partnerships and new collaborations with strong international institutions should be created or visibly strengthened every year; with at least 2-3 new institutions joined.

Visibility activities undertaken in the form of organization of international research events, such as conferences or workshops, or at least participation in the organization of such events; with 1-3 events per year. Dissemination through more prestigious means such as invited talks, tutorials, or lectures to either renowned institutions or to research gatherings should be a constant endeavor, with 2-5 such activities per year.

One infrastructure that our group is strongly involved in is the NCR. One goal is to connect the NCR to existing infrastructures and labs at NTNU that provide a test-bed for modern systems, e.g., with the Smart Grid Lab or IoT labs. Plans are to expand the NCR also with activities involving cyber-physical systems, i.e., tangible devices or their digital twins. Contributions in this direction should also come from the S2G Playground in the form of student training in ethical hacking.